HOMEWORK 1 — CS 818A4 — SPRING 2004

Problem 1

Give a formal proof of the valid assertion

$$\Big((\mathsf{x} \mapsto \mathsf{y} \ * \ \mathsf{x}' \mapsto \mathsf{y}') \ * \ \mathbf{true}\Big) \Rightarrow \Big(((\mathsf{x} \mapsto \mathsf{y} \ * \ \mathbf{true}) \wedge (\mathsf{x}' \mapsto \mathsf{y}' \ * \ \mathbf{true})) \wedge \mathsf{x} \neq \mathsf{x}'\Big)$$

from the rules on page 51 of Chapter 2 of the class notes, and (some of) the following inference rules for predicate calculus:

$$p \Rightarrow \mathbf{true} \qquad p \Rightarrow p \qquad p \wedge \mathbf{true} \Rightarrow p$$

$$\frac{p \Rightarrow q \qquad q \Rightarrow r}{p \Rightarrow r} \quad \text{(trans impl)}$$

$$\frac{p \Rightarrow q \qquad p \Rightarrow r}{p \Rightarrow q \wedge r} \quad (\wedge\text{-introduction})$$

Your proof will be easier to read if you write it as a sequence of steps rather than a tree. In the inference rules, you should regard $*$ as left associative, e.g.,

$$e_1 \mapsto e_1' \ * \ e_2 \mapsto e_2' \ * \ \mathbf{true} \Rightarrow e_1 \neq e_2$$

stands for

$$(e_1 \mapsto e_1' \ * \ e_2 \mapsto e_2') \ * \ \mathbf{true} \Rightarrow e_1 \neq e_2.$$

For brevity, you may weaken $\Leftrightarrow$ to $\Rightarrow$ when it is the main operator of an axiom. You may also omit instances of the axiom schema $p \Rightarrow p$ when it is used as a premiss of the monotonicity rule.

Problem 2

None of the following axiom schemata are sound. For each, given an instance which is not valid, along with a description of a state in which the instance is false.

$$p_1 \ * \ p_2 \not\Rightarrow p_1 \wedge p_2$$

$$p_1 \wedge p_2 \not\Rightarrow p_1 \ * \ p_2$$

$$(p_1 \ * \ p_2) \vee q \not\Rightarrow (p_1 \vee q) \ * \ (p_2 \vee q)$$

$$(p_1 \vee q) \ * \ (p_2 \vee q) \not\Rightarrow (p_1 \ * \ p_2) \vee q$$

$$(p_1 \ * \ q) \wedge (p_2 \ * \ q) \not\Rightarrow (p_1 \wedge p_2) \ * \ q$$

$$(p_1 \ * \ p_2) \wedge q \not\Rightarrow (p_1 \wedge q) \ * \ (p_2 \wedge q)$$

$$(p_1 \wedge q) \ * \ (p_2 \wedge q) \not\Rightarrow (p_1 \ * \ p_2) \wedge q$$

$$\big(\forall x.\ (p_1 \ * \ p_2)\big) \not\Rightarrow (\forall x.\ p_1) \ * \ p_2 \quad \text{when } x \text{ not free in } p_2$$

$$(p_1 \Rightarrow p_2) \not\Rightarrow \big((p_1 \ * \ q) \Rightarrow (p_2 \ * \ q)\big)$$

$$(p_1 \Rightarrow p_2) \not\Rightarrow (p_1 \mathrel{-\!\!*} p_2)$$

$$(p_1 \mathrel{-\!\!*} p_2) \not\Rightarrow (p_1 \Rightarrow p_2)$$

Problem 3

Fill in the postconditions in

$$\{(e_1 \mapsto -) \ * \ (e_2 \mapsto -)\}\ [e_1] := e_1' \ ; [e_2] := e_2' \ \{?\}$$

$$\{(e_1 \mapsto -) \wedge (e_2 \mapsto -)\}\ [e_1] := e_1' \ ; [e_2] := e_2' \ \{?\}.$$

to give two sound inference rules describing a sequence of two mutations. Your postconditions should be as strong as possible.

Give a derivation of each of these inference rules, exhibited as an annotated specification.